

UNITED STATES PATENT APPLICATION

for

**A METHOD AND APPARATUS FOR
PRESERVING CONFIDENTIALITY OF ELECTRONIC MAIL**

Inventor:

Rajasekhar Sistla

Prepared by:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026
(408) 720-8598

Attorney Docket: 42390.P10212

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number EL627471035US Date of Deposit May 8, 2001

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner for Patents, Washington, D. C. 20231.

Kelli A. Ivey

(Name of person mailing paper/fee)

Kelli A. Ivey

(Signature of person mailing paper/fee)

Date Signed: 5/8/2001

A METHOD AND APPARATUS FOR PRESERVING CONFIDENTIALITY OF ELECTRONIC MAIL

FIELD OF THE INVENTION

[0001] This invention relates to security technologies generally and particularly to their applications to electronic mails.

BACKGROUND OF THE INVENTION

[0002] Electronic mail (hereinafter email) has become a popular and in some cases, indispensable, communication tool for individuals and organizations. Despite its effectiveness for conveying information, email also poses security risks due to its inherent private or even confidential nature. For example, assuming company A has communicated with its bankers via emails regarding a buyout of company B, inability to maintain the confidentiality of these emails could potentially terminate the transaction and adversely affect company A's competitive position in its marketplace.

[0003] Some solutions have been proposed and implemented to preserve confidentiality of an email. One solution simply notifies a recipient of an email the confidentiality nature of email and assumes that the recipient would act appropriately and protectively of the email in response. Another solution assigns a password to the content of an email so that a recipient of the email can only read the content if he or she has the proper password.

[0004] The mentioned approaches have one major shortcoming. Specifically, an author of an email under either approach has no control over the email after the transmission of the email. As a result, when the recipient redistributes the content of that email to another without following the same security procedures as the author (i.e. notifying or assigning a

password), the confidentiality of the email is no longer adequately protected. Another security breach could occur when the recipient saves the email to a floppy disk and subsequently loses the floppy disk.

[0005] As has been demonstrated, an improved method and an apparatus are needed to remedy the discussed shortcoming.

[0006] BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The present invention is illustrated by way of example and is not limited by the figures of the accompanying drawings, in which like references indicate similar elements, and in which:

[0008] **Figure 1** illustrates a system configuration that one embodiment of the present invention, an electronic mail confidentiality preserver, resides in.

[0009] **Figure 2** illustrates a block diagram of one embodiment of an electronic mail confidentiality preserver.

[0010] **Figure 3** illustrates a general purpose computer system.

[0011] **Figure 4(a)** illustrates a flow chart of one process that one embodiment of the present invention follows to prepare an electronic mail for transmission.

[0012] **Figure 4(b)** illustrates a flow chart of one process that one embodiment of the present invention follows after having received an email.

DETAILED DESCRIPTION

[0013] A method and an apparatus for preserving confidentiality of an electronic mail are disclosed. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these particular details. In other instances, well-known elements and theories such as client-server architecture, encryption and decryption technologies, multiple-thread programming, etc. have not been discussed in special details in order to avoid obscuring the present invention.

[0014] Throughout the following discussion, a machine readable medium refers to, but not limited to, a storage device, a memory device, a carrier wave, etc. The term, "electronic mail" (hereinafter email), refers to a text message that includes, but not limited to, a message header and/or an attachment. A message header often contains the subject matter, origination and destination information of an email. The origination and destination information generally refers to a user's email account information. An email server, such as mail server 104 as shown in Figure 1, is responsible for maintaining such email account information and also for delivering an email to its destination based on the aforementioned destination information. On the other hand, an email client, such as sender 100 and recipient 102 as shown in Figure 1, is mostly responsible for providing its users with capabilities to manipulate an email. Some examples of such capabilities are, but without limitation, reading, editing, creating, sending and storing an email.

[0015] An email client interacts with its user through user interface 110 and communicates with its mail server or authentication server through communication engine 112.

Communication engine 112 adopts appropriate communication protocols so that its email client can establish and maintain connections with the corresponding servers. Additionally,

an email client often includes local storage 114, such as a hard disk drive, floppy drive, a removable drive, etc. to store copies of emails. An email client can then access and manipulate these stored emails without having to maintain a connection with its mail server.

[0016] In conjunction with Figure 1, the following sequence of exchanges further demonstrates the relationships among sender 100, recipient 102 and mail server 104 and the traveling path of an email from one email client to another. This example assumes that user A and user B have their email accounts with the same mail server 104, and user A uses sender 100 and user B uses recipient 102 to access their emails. In addition, user A and user B gain access to their email accounts after a successful verification of their identity information, such as, but not limited to, personal information, system password, etc. by authentication server 106.

[0017] User interface 110 of sender 100 provides user A with a text editor and a number of menu options. User A composes an email that is intended for user B with the text editor. The message header of the email contains both the previously mentioned origination information, such as user A's email account information (A@this_domain.com), and the destination information, such as user B's email account information (B@this_domain.com).

[0018] a. Then in response to user A's selection from one of the menu options to send the email, communication engine 112 of sender 100 relays A@this_domain.com, B@this_domain.com, and the content of the email to mail server 104.

[0019] b. Mail server 104 formats and stores the information that it has received in a file for user B (or hereinafter user_B_file).

[0020] c. After user B gains access to mail server 104 via recipient 102, recipient 102 requests mail server 104 for a copy of user_B_file on behalf of user B through communication engine 112.

[0021] d. Recipient 102 parses user_B_file for display via its user interface 100.

[0022] In one embodiment of the present invention, or email confidentiality preserver (hereinafter ECP) 108 as shown in Figure 1, ECP 108 resides within sender 100 and recipient 102. Alternatively, ECP 108 may reside in a standalone apparatus that is coupled to either sender 100 or recipient 102. ECP 108 primarily provides security services for sender 100 and recipient 102.

[0023] Figure 2 illustrates a block diagram of one embodiment of ECP 108. In particular, ECP 108 contains input-processing engine 200 and encryption/decryption engine 202. Before sender 100 transmits an outgoing email to mail server 104, input-processing engine 200 formats the email according to user input information 204 of the email. On the other hand, after recipient 102 receives an incoming email, either through communication engine 112 or from local storage 114, input-processing engine 200 might assert control signal 206 to disable certain options of user interface 110 and/or assert control signal 208 to invoke encryption/decryption engine 202. Subsequent sections will discuss the assertion of these control signals and the formatting of the email in more details.

[0024] Some examples of sender 100, recipient 102, mail server 104 and authentication server 106 are, but not limited to, add-in circuit boards, standalone electronic apparatuses and general-purpose computer systems. A general-purpose computer system 300 is illustrated in Figure 3.

[0025] The general-purpose computer system architecture comprises microprocessor 302 and cache memory 306 coupled to each other through processor bus 304. Sample computer system 300 also includes high performance system bus 308 and standard I/O bus 328. Coupled to high performance system bus 308 are microprocessor 302 and system controller 310. Additionally, system controller 310 is coupled to memory subsystem 316 through

channel 314, is coupled to I/O controller hub 326 through link 324 and is coupled to graphics controller 320 through interface 322. Coupled to graphics controller is video display 318. Coupled to standard I/O bus 328 are I/O controller hub 326, mass storage 330 and alphanumeric input device or other conventional input device 332.

[0026] These elements perform their conventional functions well known in the art. Moreover, it should have been apparent to one ordinarily skilled in the art that computer system 300 could be designed with multiple microprocessors 302 and may have more components than that which is shown. Also, mass storage 320 may be used to provide permanent storage for the executable instructions of ECP 108 and as local storage 114 in one embodiment, whereas memory subsystem 316 may be used to temporarily store the executable instructions during execution by microprocessor 302.

Operations of an Email Confidentiality Preserver

[0027] Figure 4(a) describes a flow chart of one process that one embodiment of ECP 108 follows to prepare an email for transmission. Specifically, using Figure 1 and the same example involving user A and user B as discussed above, user interface 110 of one embodiment of sender 100 provides user A with varying confidentiality levels to select from. For example, user interface 110 could include a menu with three confidentiality levels: high, medium and low. In response to the level that user A selects for a particular outgoing email in block 400, or user input information 204 as shown in Figure 2, input-processing engine 200 formats the outgoing email in block 402.

[0028] More particularly, one embodiment of input-processing engine 200 sets an alert flag that indicates the selected confidentiality level, appends the alert flag to the email and presents the formatted email to communication engine 112. In one implementation, the alert

flag contains a numerical value that corresponds to a confidentiality level. A “high” confidentiality level may correspond to number 3, “medium” to 2 and “low” to 1. It should however be apparent to one with ordinary skill in the art to utilize any integer number of confidentiality levels and to assign any numerical value to each of these levels, as long as one level is distinguishable from another, to implement the present invention.

[0029] Figure 4(b) illustrates a flow chart of one process that one embodiment of ECP 108 follows after its email client receives an email. Thus, in conjunction with Figures 1 and 2, after recipient 102 receives an email via its communication engine 112, input-processing engine 200 extracts the user-selected confidentiality level from the aforementioned alert flag in block 404. If the extracted information satisfies a confidentiality threshold in block 406, input-processing engine 200 then asserts control signal 206 in block 408, which causes user interface 110 to limit user B’s ability to manipulate the received email. For instance, user interface 110 may disable certain menu options and their associated keystroke shortcuts that are initially available to user B. Some examples are, but not limited to, “save to disk”, “copy/cut”, “forward”, etc. User interface 110 may also prevent user B from editing the content of the received email, replying the email with the content intact, removing confidentiality setting of the email, etc.

[0030] The confidentiality threshold mentioned above can be a numerical value that input-processing engine 200 predefines. Using the same numbering scheme discussed above (i.e. high confidentiality level = 3, medium = 2 and low = 1) as an illustration, input-processing engine 200 may preset a confidentiality threshold at 2 and assert control signal 206 if the confidentiality level of the received email exceeds 2. It should however be apparent to one of ordinary skill in the art to use a different numbering scheme and to impose a different

condition for satisfying confidentiality threshold than the one disclosed above without exceeding the scope of the present invention.

[0031] Furthermore, one embodiment of input-processing engine 200 could also assert a confidentiality-level-dependent control signal 206. More specifically, input-processing engine 200 could perform the following:

Action	Confidentiality level of a received email	Consequences
Assert one distinct control signal 206	3	Disable <i>all</i> the options in user interface 110 that could be disabled by control signal 206
Assert another distinct control signal 206	2	Disable <i>some</i> of the options in user interface 110 that could be disabled by control signal 206
Assert yet another distinct control signal 206	1	All the options in user interface 100 remain available

[0032] In block 410, input-processing engine 200 looks for attempts by its email client to access local storage 114 as shown in Figure 1 and Figure 2. In one embodiment, user interface 110 informs input-processing engine 200 of such an attempt via input information 204. Any of the following actions by a user, but not limited to, would trigger user interface 110 to notify input-processing engine 200: selecting the “export” option, selecting “save to

disk" option, copying a folder that contains received emails to local storage 114, etc. If an attempt to access local storage 114 is established, input-processing engine 200 proceeds to assert control signal 208 in block 412, which invokes encryption/decryption engine 202.

[0033] Although block 406 precedes block 410 in Figure 4(b), an ordinarily skilled artisan can practice the present invention without following that illustrated sequence. For example, the ordinarily skilled artisan may implement input-processing engine 200 using multiple threads. Particularly, one thread executes instructions for blocks 404, 406 and 408, and the other thread executes instructions for blocks 410 and 412. Either thread can proceed without waiting for the completion of the other thread's execution.

[0034] In response to the asserted control signal 208, one embodiment of encryption/decryption engine 202 prompts its user for some identity information via user interface 110. One such identity information is the user's system password, which uniquely identifies the user's email client. If the attempted access to local storage 114 in block 410 were to store information, encryption/decryption engine 202 then encrypts the email that was involved in the attempted access using the obtained identity information. On the other hand, if the attempted access were to retrieve information, then encryption/decryption engine 202 uses the identity information from its user to decrypt the email. In other words, ECP 108 ensures that any emails or folders containing emails that are stored in local storage 114 are further protected by the identity information of its user. Also, it should be noted that encryption/decryption engine 202 may utilize any existing or future encryption/decryption standards and yet still remain within the scope of the present invention.

[0035] Thus, a method and an apparatus for preserving confidentiality of an electronic mail have been disclosed. Although an email confidentiality preserver has been described particularly with reference to the figures and to specific examples, it will be apparent to one

of ordinary skill in the art that the email confidentiality preserver may appear in any of a number of other system configurations. It is further contemplated that many changes and modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the present invention.